REMARKS

The Applicant appreciates and would like to thank Examiner Syed Zia for taking time out of his schedule to discuss the subject application on 7 October 2010 with the Applicant's representative, Mr. Jeffrey J. Barclay (Reg. No. 48,950). Along with discussing the current action, the pending claims and the art reference cited in the action were also discussed.

Claims 1-12 are pending in this application, with claims 1, 7 and 11 being independent. Independent claims 1, 7 and 11 have been amended based upon the discussion with Examiner Zia. No new matter has been added by way of these amendments. Favorable reconsideration and further examination of the action is respectfully requested in view of the foregoing amendments and following comments of the Applicant, which are preceded by related comments of the Examiner in small bold type:

Claim Rejections - § 102

Claims 1-12 are rejected under 35 U.S.C. 102(e) as being anticipated by Challener et al. (U.S. Patent 6,718,468).

Amended claim 1 is directed to a computer-implemented method for a secure transaction that includes generating a first key from a user-supplied unencrypted password provided by a user computing device. The method also includes encrypting the user-supplied unencrypted password using the first key, and creating a user record. The method also includes storing the encrypted password in the user record.

Challener is understood to describe a data security technique in which unique user public/private key pairs are established for each application of a computer system. In this regard, Challener states:

> Each user of computer system 10 has a separate and unique user public/private key pair established for each application within computer system 10. The term "user" is understood to mean a person, a service, an application, a device, or any other entity that may access an application. The term "user" is not limited to a human user. A certificate may be established within computer system 10 for a user to access a particular application. The certificate may be specifically established for and associated with a particular user and a particular application. The certificate preferably includes a pointer to

> its associated application, an identity of the user associated with this certificate, and a pointer to the user private key associated with the user of this certificate and application. When an application needs to transmit an encrypted message or to perform an authentication procedure, encryption/decryption engine 32 accesses the user private key pointed to by the application's associated certificate, and then encrypts the message or signs a signature utilizing the user private key. (Col. 3, line 55 to col. 4, line 6)

Challener further describes that the public/private key pairs are received from a chip (referred to as a signature chip). As such, the reference is not understood to disclose or suggest "generating a first key from a user-supplied unencrypted password" as required by amended independent claim 1. Furthermore, rather than being user-supplied, Challener describes that a user password is randomly produced. In this regard, Challener states:

> With reference now to FIG. 2a, there is illustrated a high-level logic flow diagram of a method for associating a password with a secured user public/private key pair, in accordance with a preferred embodiment of the present invention. Starting at block 40, a user public/private key pair is first received by a signature chip (such as signature chip 31 from FIG. 1), as shown in block 41. Typically, this user public/private key pair has already been certified with the proper authority. A random password, preferably 64 bits in length, to be associated with the user public/private key pair is then generated for the user, as depicted in block 42. This random password, which is preferably generated by a random generator, is typically very difficult for a human user to remember. Utilizing a chip public key, the random password is then encrypted along with the user public/private key pair, as shown in block 43. The chip public key may come from an unprotected or protected storage area of the signature chip. The encrypted package of the random password and user public/private key pair is then stored in a hard disk, such as SCSI disk drive 19 as shown in FIG. 1. At this point, any record of the user public/private key pair outside the signature chip can be discarded (by the human user) for security reasons, as depicted in block 44. (Col. 4, lines 7-29; emphasis added)

Thus, rather than being user-supplied, a password is generated (preferably with a random generator) for a user. As such, along with being silent in regards to using a user-supplied unencrypted password to generate a first key, the reference does not disclose or suggest a password that is user-supplied.

For at least these reasons, amended independent claim 1 is believed to be patentable over the Challener reference. Similarly, amended independent claims 7 and 11 are also believed to be allowable for at least the same reasons noted above. The dependent claims 2-6, 8-10 and 12 respectively partake of the novelty of their parent independent claims and, as such, have not been addressed specifically herein.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

In view of the foregoing remarks, the entire application is now believed to be in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience. Applicants' attorney can be reached at the address shown below. Telephone calls regarding this application should be directed to 617-368-2191.

The fee of $245 for the petition for extension of time is being paid concurrently herewith on the Electronic Filing System (EFS) by way of Deposit Account Authorization. Please apply any other charges or credits to deposit account 06 1050, referencing Attorney Docket No. 13984-0005US1.

Respectfully submitted,

Date: 22 October 2010

Jeffrey J. Barclay
Reg. No. 48,950

Customer Number 26161
Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945